SIGNAL

CAPITAL

MANUAL DE COMPLIANCE

2023

SIGNAL
CAPITAL

ÍNDICE

SIGNAL
CAPITAL

MANUAL DE CONDUTA E ÉTICA

ÍNDICE

O objetivo deste Código de Ética é descrever as normas e os procedimentos a serem observados pelos quotistas, sócios, diretores, gerentes e funcionários da Signal Capital Investimentos Ltda. ("Signal Capital") ("Funcionários", quando no plural, ou "Funcionário" quando no singular, sem distinção) no exercício de suas atividades, a fim de assegurar a observância contínuas dos regulamentos em vigor e com os mais altos padrões de conduta ética nos negócios.

PRINCÍPIOS GERAIS E NORMAS DE CONDUTA ÉTICA

Este Código de Ética aplica-se a todos os funcionários da Signal Capital. Em caso de dúvida sobre como o Código de Ética se aplica a situações específicas, os funcionários devem consultar o Diretor de Compliance, Prevenção à Lavagem de Dinheiro e Gestão de Riscos da Signal Capital ("Diretor de Compliance") conforme necessário, especialmente com relação a questões que envolvem a regulamentação vigente.

O Diretor de Compliance, é responsável por supervisionar as atividades da Signal Capital e o desempenho de todos os seus Funcionários, bem como pela administração geral das políticas e procedimentos estabelecidos neste Código de Ética. O Diretor de Compliance revisará todos os relatórios relacionados a este Código de Ética e o atualizará conforme necessário.

O Diretor de Compliance, também é responsável por revisar periodicamente a adequabilidade e eficácia das políticas e procedimentos aplicados neste Código de Ética.

O Departamento de Compliance deve investigar qualquer possível violação das políticas e procedimentos estabelecidos nesse Código de Ética e determinar as sanções que podem ser impostas.

Periodicamente, o Diretor de Compliance tomará as devidas medidas de modo a assegurar a conformidade da Signal Capital com todas as normas e procedimentos exigidos pela regulamentação brasileira.

PRINCÍPIOS E PADRÕES DE CONDUTA E ÉTICA A SEREM ADORATOS

Tendo em vista a relação de confiança entre a Signal Capital e seus clientes, e considerando que a Signal Capital tem o dever de agir em nome de e de acordo com os melhores interesses de seus

clientes, os seguintes princípios gerais devem orientar a conduta dos Funcionários da Signal Capital no exercício das suas funções:

I. Os Funcionários abster-se-ão de agir de forma que viole os regulamentos e leis em vigor;

II. Os Funcionários devem aderir aos mais altos padrões de conduta ética no exercício das suas atividades na Signal Capital ou quando agirem em seu nome;

III. Os Funcionários devem manter a confidencialidade de todas as informações obtidas no exercício das suas atividades na Signal Capital;

IV. Os Funcionários devem informar ao Diretor de Compliance a respeito de qualquer fato que possa ser considerado potencialmente prejudicial à Signal Capital, incluindo possíveis violações das normas e procedimentos estabelecidos neste Código de Ética e não devem, de forma alguma, apoiar ou tolerar qualquer ato em violação dos regulamentos e leis aplicáveis;

V. Os Funcionários abster-se-ão de fazer uso indevido dos ativos financeiros pertencentes à Signal Capital e/ou seus clientes com a finalidade de obter qualquer benefício, quer pessoal e/ou para terceiros;

VI. Os Funcionários devem revelar quaisquer atividades que possam criar um conflito de interesse, atual ou potencial, entre qualquer funcionário, a Signal Capital e/ou seus clientes;

VII. Os Funcionários devem lidar de forma justa e equitativa com os clientes da Signal Capital e não devem abusar da confiança de que gozam em virtude de representar a Signal Capital para obter vantagens indevidas para si mesmos ou para terceiros; e

VIII. Os Funcionários deverão aderir a todos os termos deste Código de Ética e permitir o monitoramento do cumprimento integral pelo Departamento de Compliance.

CONFLITO DE INTERESSE

A Signal Capital reconhece que podem surgir conflitos de interesse com relação ao fornecimento de serviços de investimento e, em particular, no que diz respeito à alocação das oportunidades de investimento entre os clientes e/ou fundos da Signal Capital. Todos esses conflitos de interesse devem ser analisados e resolvidos de acordo com a seguinte política:

I. A Signal Capital alocará oportunidades de investimento entre todos os clientes e fundos gerenciados, de acordo com sua política de alocação interna, levando em consideração o tamanho de cada conta e/ou fundo, o montante global disponível à Signal Capital para um

determinado investimento, a estratégia de investimento dos clientes e fundos aplicáveis, a constituição do portfólio da conta e/ou fundo no momento do investimento, e outros fatores, conforme os agentes responsáveis por essa alocação considerarem relevantes sob as circunstâncias; e

II. A Signal Capital deve considerar, em todos os momentos, suas obrigações contratuais e de lealdade para com todos os clientes e fundos gerenciados, reconhecendo que, por vezes, pode haver interesses concorrentes, o que deve ser equilibrado. A Signal Capital alocará investimentos entre seus clientes de acordo com sua política de alocação interna. Além disso, a Signal Capital não deve alocar as oportunidades de investimento com base, como um todo ou em parte, na remuneração paga por qualquer cliente ou fundo ou na rentabilidade de qualquer conta ou fundo.

Além disso, todos os relatórios de pesquisa de valores mobiliários produzidos por analistas da Signal Capital não devem ser tendenciosos e devem ser imparciais.

CONFLITOS PESSOAIS E PRESENTES

Os Funcionários devem evitar situações em que seus interesses pessoais possam estar ou parecer estar em conflito com os interesses da Signal Capital. Podem surgir conflitos de interesse quando a posição ou as responsabilidades para com o cliente e/ou a Signal Capital apresentarem uma oportunidade para ganho pessoal além da compensação normal dada através do vínculo empregatício.

As seguintes diretrizes foram desenvolvidas para auxiliar os funcionários a evitarem possíveis conflitos de interesse:

I. **Utilização de Recursos e Ativos Corporativos:** Os ativos da Signal Capital incluem não só mobiliário, equipamentos e suprimentos de escritório, mas também lista de clientes, materiais de marketing, estratégias e planos de negócios, processos de diligência, estratégias de investimento e outras informações sobre o negócio. Os Funcionários estão proibidos de utilizar esses ativos para ganho pessoal e de fornecer qualquer um desses ativos a terceiros sem autorização prévia e expressa. O furto de dinheiro, propriedade ou outros ativos da Signal Capital não será tolerado;

II. **Informações Confidenciais:** Funcionários terão acesso, de forma rotineira, a informações confidenciais sobre a Signal Capital, seus clientes, prestadores de serviços, e outras partes com quem a Signal Capital faz negócios. Enquanto tais informações permanecerem confidenciais, não devem ser divulgadas a outros funcionários que não tenham necessidade de conhecê-las ou a pessoas que não são funcionárias, por qualquer razão, exceto em

conformidade com procedimentos estabelecidos. A maioria das informações financeiras e outras informações relacionadas aos clientes e suas carteiras de investimento estão sujeitas a seus direitos legais de privacidade. Além disso, os clientes da Signal Capital estão cientes das restrições de confidencialidade com relação a as informações que recebem dos fundos e empresas da carteira em que investiram, e os funcionários devem presumir que estas restrições se aplicam também à Signal Capital. É imperativo que todos os funcionários cumpram essas políticas de confidencialidade de forma rigorosa a fim de proteger os direitos de seus clientes. O dever de proteger as informações confidenciais da Signal Capital e de seus clientes inclui evitar qualquer divulgação intencional, bem como não intencional e indireta.

III. **Alocação de Investimentos:** A alocação de oportunidades de investimento aos clientes da Signal Capital envolve potenciais conflitos de interesse. A Signal Capital adotou políticas e procedimentos para evitar esses conflitos, conforme estabelecidos nos Manuais e na Políticas da Signal Capital. A Signal capital não alocará oportunidades de investimento com base na estrutura da taxa ou no valor das taxas pagas por qualquer cliente ou fundo ou na rentabilidade de qualquer cliente ou fundo, conforme descrito acima;

IV. **Atividades Externas:** Os Funcionários devem evitar empregos ou atividades externas que possam ter impacto negativo sobre seu desempenho no trabalho na Signal Capital ou que possam gerar conflito ou a aparência de conflito com suas obrigações perante a Signal Capital. Os funcionários não podem se envolver em atividades pessoais que estejam em conflito com os melhores interesses da Signal Capital ou de seus clientes, incluindo, mas não limitado a trabalhar para um concorrente da Signal Capital. Devido à natureza fiduciária do negócio da Signal Capital, todos os potenciais conflitos de interesse que poderiam resultar de emprego externo ou de outras atividades externas de um funcionário devem ser discutidos com as áreas responsáveis; e

V. **Oportunidades Corporativas:** Todas as oportunidades de negócios para investimentos pessoais que cheguem à atenção de qualquer funcionário que de alguma forma se relacionem aos negócios da Signal Capital são consideradas "oportunidades corporativas". Os Funcionários estão proibidos de utilizar sua posição na Signal Capital para se apropriar, quer para seja para si mesmo ou para qualquer afiliado ou membro da família, de oportunidades de negócios que pertençam por direito à Signal Capital, quer tais oportunidades sejam descobertas ou não através da utilização de bens ou informações da Signal Capital ou no exercício das suas funções.

Presentes de valores significativos podem pressionar Funcionários a prestar favores ou podem dar a aparência de um conflito de interesses. Os funcionários não podem, em nenhum momento, aceitar qualquer item que esteja condicionado à Signal Capital fazer negócios com a entidade ou pessoa

que dá o presente. Presentes em dinheiro, gratificações, bônus, taxas ou comissões de qualquer valor nunca devem ser aceitos. Os funcionários não podem aceitar ou receber presentes não monetários ou qualquer outra forma similar de retribuição, quer direta ou indiretamente, de qualquer pessoa ou empresa com a qual Signal Capital faz ou pretende fazer negócios se o valor for superior a R$500 por ano. Além disso, os Funcionários não podem solicitar a qualquer terceiro qualquer tipo de presente ou formas semelhantes de consideração, independentemente do seu valor.

A Signal Capital pode aceitar ou participar de entretenimento razoável fornecido por qualquer pessoa ou empresa com a qual a Signal Capital faz ou pretende fazer negócios. "Entretenimento razoável" incluiria, entre outras coisas, uma refeição ocasional, um ingresso para um evento esportivo ou teatro, ou entretenimento comparável:

- que não seja nem frequente nem excessivo a ponto de levantar qualquer dúvida de adequação;
- aquela à qual a entidade ou pessoa que presenteia o entretenimento, refeição ou bilhetes compareça;
- que não seja fornecida em frequência superior a uma vez por trimestre pela mesma pessoa ou empresa; e
- que não seja condicionada à Signal Capital obter ou manter negócios.

As políticas da Signal Capital com relação a presentes e entretenimento não se aplicam apenas aos funcionários, mas também aos seus familiares imediatos.

Essas políticas não impedem diretores que não atuam em cargos de gestão na Signal Capital de aceitar qualquer compensação, bônus, taxa e outras considerações semelhantes pagos no curso normal dos negócios como resultado de sua atividade comercial, vínculo empregatício ou diretorias externas.

FALSIFICAÇÃO OU ALTERAÇÃO DE REGISTROS

Falsificar ou alterar registros ou relatórios ou preparar registros ou relatórios que não reflitam adequadamente operações ou atividades conduzidas pela Signal Capital, ou aprovar tais registros ou relatórios falsos, alterados ou preparados de forma inadequada, constitui não apenas uma violação da conduta ética conforme estabelecida neste Código de Ética, mas também pode sujeitar a Signal Capital e nossos funcionários a penalidades civis e criminais. Nenhum funcionário pode se envolver em qualquer arranjo ou operação que possa ser interpretado como uma declaração falsa ou dissimulação de sua verdadeira natureza ou propósito. São exemplos de práticas proibidas:

I. Fazer declarações falsas ou inexatas nos livros, registros ou relatórios contábeis da Signal Capital ou de seus clientes a fim de ocultar ou alterar a natureza de uma operação ou atividade;
II. Manipular livros, registros ou relatórios contábeis para ganho pessoal;
III. Não manter livros e registros contábeis que reflitam plenamente e com precisão todas as operações realizadas pela Signal Capital ou seus clientes;
IV. Não revelar quaisquer informações da Signal Capital ou de seus clientes das quais os funcionários têm conhecimento e que não tenham sido devidamente divulgadas ou registrados; e
V. Efetuar o pagamento ou dar quitação sabendo que os recursos utilizados ou recebidos serão utilizados para fins diferentes dos descritos no registro de operação.

SIGNAL
CAPITAL

POLÍTICA DE EXERCÍCIO DE DIREITO DE VOTO

OBJETIVO DA POLÍTICA

O objeto da presente política ("Política de Voto") é estabelecer as diretrizes que disciplinarão o exercício, pela Signal Capital Investimentos Ltda. ("Signal Capital" ou "Signal" ou "Gestora"), do direito de voto em assembleias gerais ("Assembleias Gerais") dos cotistas, acionistas ou debenturistas, conforme o caso, dos Fundos Alvo, das Sociedades Alvo ou carteiras geridas pela Signal Capital Investimentos, bem como aquelas nas quais a Signal Capital atue como órgão consultivo, desde que a titularidade de tais ativos contemple o direito de voto em Assembleias Gerais, em conformidade com a Instrução CVM 578 e Código ABVCAP / ANBIMA de Regulação e Melhores Práticas para o Mercado de FIP e FIEE.

A política de voto do Gestor destina-se a orientar a participação do Gestor em todas as assembleias gerais dos emissores de títulos e valores mobiliários que confiram direito de voto aos fundos de investimento sob sua gestão, nas hipóteses previstas em seus respectivos regulamentos e quando na pauta de suas convocações constarem as matérias relevantes obrigatórias descritas na referida política de voto. Ao votar nas assembleias representando os fundos de investimento sob sua gestão, o Gestor buscará votar favoravelmente às deliberações que, a seu ver, propiciem a valorização dos ativos financeiros que integrem a carteira do fundo de investimento.

A presente Política de Voto não será aplicável na seguinte hipótese:

I. qualquer Fundo gerido pela Signal Capital Investimentos que expressamente descreva em seu regulamento a dispensa de cumprimento com esta Política de Voto;

PRINCÍPIOS GERAIS DA POLÍTICA DE VOTO

Na qualidade de representante dos Fundos, das carteiras que possuam a Signal Capital como órgão consultivo e/ou dos Fundos ou carteiras sob sua gestão, a Signal Capital deverá exercer seu direito de voto em Assembleias Gerais de acordo com os melhores interesses dos referidos Fundos e de seus quotistas ("Quotistas"), bem como das referidas carteiras. A Signal Capital Investimentos define "melhores interesses" como melhor interesse econômico dos quotistas ou dos clientes associados às referidas carteiras.

Em qualquer caso, a Signal Capital fará o possível para exercer o direito de voto nas Assembleias Gerais nos melhores interesses dos Quotistas e dos clientes associados às referidas carteiras. No exercício de seu direito de voto, a Signal Capital levará em conta fatores que a Equipe de Investimentos e eventuais Comitês Consultivos dos Fundos considerem aplicáveis para os interesses econômicos dos quotistas e/ou dos clientes, incluindo, mas não se limitando, as diretrizes de

investimento de determinado Fundo ou cliente, o estado atual do cliente ou da carteira do Fundo, as práticas e condições atuais de mercado (ou seja, se a realização ou não de um determinado aditamento ou a adoção de determinadas ações é consistente com os termos então em vigor ou com a prática usual de fundos ou empresas similares), e o desempenho financeiro de tal investimento. No caso de co-investimentos, os acionistas das companhias que fazem parte da carteira gerida pela Signal Capital, geralmente fazem parte de acordos de acionistas, os quais regulamentam as formas pelas quais tais acionistas devem votar no que diz respeito a questões específicas. Em tais casos, a Signal Capital será obrigada a votar em conformidade com referidos acordos.

Tendo em vista que existem diversos fatores que influenciam o exercício do direito de voto e que existem vários tipos de questões e matérias sobre as quais os Emissores poderão requerer alterações ou aprovações prévias, a Signal Capital não estabeleceu uma lista de questões "típicas" a respeito das quais votará a favor ou contra.

A política da Signal Capital é analisar cada proposta de acordo com os seus próprios méritos, levando em consideração todos os fatores relevantes, não adotando regras inflexíveis com relação a qualquer questão específica que possa vir a ser colocada sob votação.

A Signal Capital deverá, no exercício do direito de voto de que trata o item acima, (i) empregar todo o cuidado e a diligência que o homem ativo e probo costuma dispensar à administração de seus próprios negócios, (ii) atuar com lealdade em relação aos interesses dos Quotistas e clientes, e (iii) envidar seus melhores esforços para evitar quaisquer práticas que possam ferir a relação de fidúcia mantida entre a Signal Capital e os Quotistas ou seus clientes.

As decisões de voto serão tomadas com base na situação do mercado quando do momento do voto, em informações divulgadas ao mercado e/ou disponibilizadas pelos Emissores, bem como na estratégia de investimento da Signal Capital para o respectivo Fundo ou carteira.

A Signal Capital utilizará seu voto para, sempre que possível, valorizar os ativos integrantes das carteiras dos Fundos e demais carteiras sob sua gestão ou nas quais a Signal Capital atue como órgão consultor.

EXERCÍCIO DO DIREITO DE VOTO

O exercício do direito de voto pela Signal Capital deve estar de acordo com as orientações fornecidas pela Equipe de Investimentos, pelo Comitê de Investimentos e por qualquer Comitê Consultivo dos Fundos, caso aplicável.

Sem prejuízo das exceções previstas no item acima, é obrigatório o exercício do voto, pela Signal Capital, nos seguintes casos ("Matérias Relevantes Obrigatórias"):

No caso de ações, seus direitos e desdobramentos:

I. eleição de representantes de sócios minoritários nos Conselhos de Administração, se aplicável;
II. aquisição, fusão, incorporação, cisão, alterações de controle, reorganizações societárias, alterações ou conversões de ações e demais mudanças de estatuto social, que possam, no entendimento da Signal Capital, gerar impacto relevante no valor do ativo detido pelo Fundo; e
III. demais matérias que impliquem tratamento diferenciado;

No caso de ativos financeiros de renda fixa ou mista, alterações de prazo ou condições de prazo de pagamento, garantias, vencimento antecipado, resgate antecipado, recompra e/ou remuneração originalmente acordadas para a operação; e

No caso de quotas de fundos de investimento:

I. alterações na política de investimento que alterem a classificação do fundo nos termos da regulamentação da Comissão de Valores Mobiliários ou o tipo do Fundo, conforme código ABVCAP/ANBIMA;
II. mudança de administrador ou gestor, que não entre integrantes do seu conglomerado ou grupo financeiro;
III. aumento de taxa de administração ou criação de taxas de entrada e/ou saída;
IV. alterações nas condições de resgate que resultem em aumento do prazo de saída;
V. fusão, incorporação ou cisão, que propicie alteração das condições elencadas nas alíneas anteriores;
VI. liquidação do fundo de investimento; e
VII. assembleia de quotistas nos casos previstos da Instrução CVM nº 578/16

É obrigatório o exercício do direito de voto pela Signal Capital em relação às matérias descritas no item acima, exceto nos seguintes casos, em que o exercício do direito de voto ficará a exclusivo critério da Signal Capital:

I. a Assembleia Geral ocorrer em qualquer cidade que não seja capital de Estado e não seja possível votar à distância;
II. o custo decorrente do exercício do voto não for compatível com a relevância do ativo objeto do direito de voto na composição da carteira do Fundo;
III. a participação total do Fundo e/ou das carteiras geridas pela Signal Capital ou dos Fundos e carteiras em que a Signal Capital atue como órgão consultivo no ativo objeto da Política de Voto seja inferior a 5% (cinco por cento) ou nenhum Fundo e/ou carteiras geridas pela Signal

Capital ou nas quais a Signal Capital atue como órgão consultivo possua mais que 10% (dez por cento) de seu patrimônio investido no ativo em questão;

IV. houver um potencial conflito de interesses, observado o disposto no item III; e

V. se as informações disponibilizadas pelo Emissor não forem suficientes, mesmo após solicitação de informações adicionais e esclarecimentos, para a tomada de decisão pela Signal Capital.

VI. Se a posição da Signal Capital já estiver definida em outro documento ou acordo, incluindo, mas não se limitando a acordo de acionistas.

Observado o exercício de direito de voto em relação às matérias descritas no item acima, é facultado à Signal Capital comparecer às Assembleias Gerais, bem como exercer o direito de voto em relação a outras matérias que, a seu critério, sejam de interesse dos Fundos e/ou dos Quotistas.

A Equipe de Investimentos tem a responsabilidade de votar em deliberações referentes aos valores mobiliários sobre os quais a Signal Capital tem autoridade discricionária. Tanto o documento físico do voto quanto a versão digital serão armazenadas pela Gestora.

DOS PROCEDIMENTOS EM SITUAÇÕES DE POTENCIAL CONFLITO DE INTERESSE

Sempre que surgir um conflito de interesses entre os fundos geridos pela Signal Capital e a própria Gestora, tal conflito será resolvido no âmbito da Assembleia Geral de Cotistas dos fundos envolvidos. e da Signal Capital.

DO PROCESSO DECISÓRIO, REGISTRO E FORMALIZAÇÕES DE VOTO

O controle desta Política de Voto será feito pela área de investimentos da Signal Capital Investimentos, sob responsabilidade do Gestor da Signal, identificado abaixo, conforme instruído pela Equipe de investimentos da Signal Capital.

As decisões relativas aos votos serão tomadas pela Signal Capital (conforme instruído pela Equipe de investimentos da Signal Capital), observados os procedimentos descritos a seguir:

I. recebimento e processamento da convocação da Assembleia Geral;

II. estudo dos assuntos indicados como ordem do dia na convocação recebida, utilizando-se das diretrizes definidas nos Princípios Gerais desta Política de Voto;

III. decisão, pela Signal Capital, do voto a ser proferido na Assembleia Geral, com antecedência mínima de 2 (dois) dias úteis em relação à data da Assembleia Geral;

IV. nomeação de um representante da Signal Capital para exercício do voto, quando for o caso.

V. Participação na Assembleia de forma presencial ou virtual e envio do voto por email ou documento físico, quando necessário.

Adicionalmente, a Signal Capital irá manter os seguintes registros:

I. cópia de cada documento (incluindo procurações, se existentes) que a Signal Capital receber relacionado a votações em nome de seus clientes ou Fundo;
II. registro de cada voto proferido pela Signal Capital Investimentos em nome de cada Fundo ou cliente;
III. cópia de cada documento elaborado pela Signal Capital que foi substancial para a tomada de uma decisão acerca de como votar em nome de um determinado cliente ou Fundo, ou que sintetize a base para tal decisão; e

A Signal Capital manterá os documentos descritos acima pelo período necessário, conforme previsto na legislação e regulamentação aplicáveis.

Observado o disposto no contrato social da Signal Capital, poderá ser nomeado como representante da Signal Capital, procurador que não faça parte do quadro de funcionários da Signal Capital.

A Signal Capital elaborará procuração por meio da qual serão outorgados poderes necessários ao representante para que o mesmo pratique todos os atos necessários para a devida representação junto à Assembleia Geral.

Os Quotistas serão informados pelo administrador do Fundo do voto proferido pela Signal Capital Investimentos por meio do extrato do Fundo referente ao mês seguinte ao do recebimento da comunicação.

O responsável pelo exercício e controle desta Política de Voto é o Sr. Ricardo Fernandez Silva Junior, brasileiro, casado, administrador de empresas, portador da Cédula de Identidade RG n.º 107350738, inscrito no CPF/MF sob o n.º 073.025.22723.

DISPOSIÇÕES GERAIS

Uma cópia desta Política de Voto será fornecida aos Quotistas e aos clientes, mediante solicitação. Além disso, cópias dos registros descritos acima que dizem respeito a um determinado Quotista ou cliente será fornecido a tal Quotista ou cliente, mediante solicitação.

SIGNAL
CAPITAL

POLÍTICA DE GERENCIAMENTO DE CIBERSEGURANÇA

OBJETIVO

A política define os requisitos básicos para prevenir, detectar e responder a riscos e ameaças de cibersegurança. O objetivo desta Política é garantir que funcionários e administradores mantenham foco adequado no nível de segurança das informações, de modo a assegurar que:

- a cibersegurança tenha prioridade máxima;
- Informação com classificação de segurança tenham proteção adequada;
- a segurança das informações, incluindo controles de cibersegurança, tenha governança efetiva;
- avaliações de risco de cibersegurança sejam parte integrante da estrutura.

PÚBLICO ALVO

Esta política se aplica a todos os funcionários e contratados da Signal Capital. Os requisitos para a proteção dos dados e das informações da Signal Capital, conforme estabelecidos nesta política, também devem ser estipulados e cumpridos sempre que terceiros (inclusive consultores, trabalhadores contingentes, contratados ou prestadores de serviços) prestarem serviços para a Signal Capital, ou em seu nome.

RESPONSABILIDADES

A Signal Capital e seus funcionários devem observar os seguintes princípios de cibersegurança:

- proteger a Signal Capital contra riscos e ameaças de cibersegurança;
- compreender e cumprir obrigações legais, regulatórias e gerenciais;
- observar os princípios de segurança, integridade e disponibilidade das informações confidenciais;
- relatar riscos residuais e de segurança das informações

A diretoria da Signal Capital é responsável por:

- definir e garantir a execução da estratégia de gerenciamento de risco de segurança das informações;

- revisar normas e políticas relevantes, para garantir que controles mínimos de segurança das informações;
- monitorar o cumprimento das políticas de segurança das informações, em parceria com o departamento de TI.

O autor é responsável por revisar e atualizar esta política conforme necessário.

MEDIDAS DISCIPLINARES

Violações desta política podem resultar em medida disciplinar, até (inclusive) demissão. Violações das obrigações legais ou regulatórias poderão ser relatadas as autoridades externas e poderão resultar em penas criminais, cíveis ou regulatórias.

PRINCÍPIOS E CONTROLES DE SEGURANÇA DA INFORMAÇÃO

Segurança das informações consiste na proteção das informações e dos sistemas de informação contra acesso, uso, divulgação, modificação ou destruição não autorizados, a fim de garantir sua confidencialidade, integridade e disponibilidade.

Esta política apresenta os princípios que devem ser seguidos para o uso aceitável e adequado de hardware, software, sistemas, aplicativos, dados, instalações e redes de tecnologia da informação, bem como equipamentos de telecomunicações com base em exigências e objetivos de controle de segurança das informações para proteger os ativos de Tecnologia da Informação da Signal Capital.

CLASSIFICAÇÃO E GERENCIAMENTO DE RISCO

As informações devem ser classificadas nos seguintes níveis: secretas, confidenciais, internas, irrestritas e públicas, de acordo com a confidencialidade e as proteções necessárias.

Contratos e/ou outras medidas adequadas devem ser firmados para a troca, a transferência, o armazenamento ou o processamento seguro dos dados classificados como internos, ou classificação superior, entre a Signal Capital e partes externas.

CONTROLE DE ACESSO

O acesso a informações deve ser restrito com base nos negócios ou nas funções que os usuários precisam desempenhar.

As contas de usuários devem ser gerenciadas de acordo com um processo definido de administração de usuários. Um identificador único deve ser designado a cada um dos usuários. Para tipos de contas de usuários que exigem senhas, deve-se definir regras de gerenciamento de senhas para cada tipo de conta.

Procedimentos devem ser estabelecidos para garantir a adição e a modificação tempestiva e específica dos acessos adequados às atribuições dos usuários. A desativação/exclusão de contas de usuário deve ser feita de forma tempestiva.

GERENCIAMENTO DE VULNERABILIDADE TÉCNICA

Controles devem ser estabelecidos para prevenção, detecção e recuperação de ameaças, tais como:

- Remoção de componentes não utilizados e sujeitos a vulnerabilidades;
- Procedimentos de bloqueio de instalação de software não padrão;
- Uso de software, ferramentas ou utilitários restritos apenas aos autorizados pela Signal Capital;
- Soluções para proteção contra malware configuradas para que monitorem continuamente os sistemas e arquivos de computador e identifiquem características da presença ou atividade de malware;
- Mecanismos para detectar acessos não autorizados a redes e serviços de rede

SEGURANÇA DAS OPERAÇÕES

Os sistemas e os aplicativos devem ser projetados para garantir que os controles de segurança das informações sejam implementados e testados e não possam ser contornados.

Os ambientes de desenvolvimento, teste e laboratório devem estar física ou logicamente separados do ambiente de produção.

Os proprietários dos sistemas devem se assegurar de que os registros de auditoria das atividades de usuários, as exceções e os eventos de segurança das informações serão produzidos pelos sistemas e retidos de forma segura por um período definido.

Cópias de back-up de informações e de softwares do ambiente de produção devem ser feitas, e a eficácia dos procedimentos de restauração deve ser testada regularmente.

TREINAMENTO E CONSCIENTIZAÇÃO SOBRE SEGURANÇÃ DA INFORMAÇÃO

Os funcionários da Signal Capital devem receber treinamento regular sobre segurança das informações e cibersegurança, conforme for adequado e relevante para as habilidades, responsabilidades e funções de cada um.

O treinamento poderá incluir:

- eLearnings;
- testes de simulação de phishing;
- conversas e palestras;
- documentos e comunicação corporativa

TRATAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Os incidentes de Segurança da Informação devem ser reportados e, quando necessário, escalados a alta gerência de forma tempestiva.

Um incidente deve ser acompanhado e monitorado durante todo o seu ciclo de vida por meio do registro de eventuais alterações em seu status ou prioridade e deve ser processado de acordo com os marcos estabelecidos no ciclo de vida do processo

Medidas devem ser tomadas para evitar que incidentes de segurança se espalhem, para proteger a Signal Capital contra futuras exposições a incidentes similares e para verificar a propagação de incidentes.

As medidas de resolução e recuperação fazem parte do registro do incidente e devem ser documentadas.

A equipe de Compliance deve ser informada sobre o gerenciamento de incidentes de segurança que infrinja efetiva ou potencialmente as leis e/ou os regulamentos locais; e deverá estar diretamente envolvida nos casos em que o relato de problemas de segurança for uma exigência legal ou regulatória.

GLOSSÁRIO

Disponibilidade – Garantia de acesso a informações e seu uso de maneira tempestiva e confiável.

Confidencialidade – Preservação das restrições autorizadas sobre o acesso a informações e sua divulgação, incluindo os meios para proteger a privacidade individual e as informações exclusivas.

Cibersegurança – O processo que consiste em proteger informações pela prevenção, detecção e resposta a ataques.

Segurança das informações – No contexto da Signal Capital, segurança das informações, que inclui cibersegurança, consiste na preservação das seguintes propriedades das informações:

- Confidencialidade
- Integridade
- Disponibilidade

Incidentes de segurança – Violação ou ameaça iminente de violação de políticas de segurança digital, políticas de uso aceitável ou práticas de segurança comuns.
Integridade – Proteção contra modificação ou destruição inapropriada de informações, o que inclui garantir o não repúdio e a autenticidade das informações.

Malware – Código malicioso que causa danos ou permite a subversão de sistemas. Exemplos tradicionais de códigos maliciosos incluem vírus, worms, Cavalos de Tróia e scripts de ataque; e os exemplos mais recentes incluem applets maliciosos em Java e controles ActiveX.

SIGNAL
CAPITAL

POLÍTICA DE PREVENÇÃO AO INSIDER TRADING

INTRODUÇÃO

Em geral, é ilegal para qualquer indivíduo, pessoalmente ou em nome de terceiros, negociar valores mobiliários com base em informações materiais não públicas. Também é geralmente ilegal comunicar informações materiais não públicas a terceiros, para que possam negociar valores mobiliários com base nessas informações. Essas atividades ilegais são comumente chamadas de "*insider trading*". As penalidades para *insider trading* incluem multas civis de até três vezes o lucro obtido ou perda evitada pela negociação, multas criminais e prisão. Também pode haver responsabilidade para aqueles que foram prejudicados pela negociação. Uma empresa cujo funcionário viola as proibições de uso de informações privilegiadas pode ser responsabilizada por uma multa civil ou três vezes o lucro ganho ou perda evitada como resultado da violação de informações privilegiadas do funcionário.

Esta política estabelece (1) as proibições legais gerais com relação ao uso de informações privilegiadas; (2) o significado dos conceitos-chave subjacentes à proibição; e (3) as sanções para negociações com informações privilegiadas. Esta política se aplica a todos os diretores, executivos e funcionários da Empresa, bem como aqueles considerados "pessoas de acesso", que inclui todas as pessoas que têm acesso a informações não públicas sobre os investimentos dos clientes ou participam de o processo de investimento.

DECLARAÇÃO SOBRE INSIDER TRADING

A Empresa proíbe qualquer um de seus diretores, executivos, funcionários ou pessoas de acesso de negociar, pessoalmente ou em nome de terceiros, com base em informações materiais não públicas ou comunicar informações materiais não públicas a terceiros em violação da lei. Essa conduta é frequentemente referida como "negociação com informações privilegiadas".

O termo "negociação com informações privilegiadas" geralmente é usado para se referir à situação em que uma pessoa negocia enquanto tem conhecimento de informações materiais não públicas ou comunica informações materiais não públicas a terceiros em violação de um dever de confiança ou segurança.

É usualmente entendido que a lei proíbe

- negociação por pessoa com acesso à informação privilegiada, enquanto tenha conhecimento de informações materiais não públicas; ou:
- negociação por uma pessoa sem acesso à informação privilegiada, enquanto tenha conhecimento de informações materiais não públicas, em que a informação foi divulgada a

uma pessoa sem acesso à informação privilegiada em violação do dever de uma pessoa privilegiada de mantê-la confidencial; ou

- comunicar informações materiais não públicas a terceiros em violação de um dever de confiança ou sigilo.

Esta política se aplica a todos os diretores, executivos, funcionários e pessoas com acesso a informação privilegiada, e se estende a atividades dentro e fora de suas funções na Empresa. Cada diretor, executivo, funcionário e pessoa com acesso à informação privilegiada deve ler e guardar esta declaração de política.

Quaisquer dúvidas com relação a esta política e os procedimentos relacionados aqui estabelecidos devem ser encaminhadas ao Diretor de Compliance.

A seguir estão descritos os elementos do uso de informações privilegiadas, as penalidades para tais condutas ilegais e os procedimentos adotados pela Empresa para implementar sua política contra uso de informações privilegiadas.

PESSOAS COBERTAS POR ESTA POLÍTICA

Esta política se aplica às Pessoas com exposição a informação privilegiada, bem como a quaisquer transações em quaisquer valores mobiliários participados por membros da família ou empresas controladas por tais pessoas. Em particular, esta política se aplica a transações de títulos por:

- o cônjuge da Pessoa exposta;
- os filhos menores da Pessoa exposta;
- quaisquer outros parentes que vivam na residência da Pessoa exposta;
- Veículo de investimento no qual a pessoa exposta seja beneficiário final e tenha algum tipo de controle direto ou indireto
- empresa da qual a Pessoa exposta é diretor ou acionista com participação de 10% ou mais; ou
- uma sociedade da qual a Pessoa exposta é vinculada (incluindo a maioria dos clubes de investimento), a menos que a Pessoa exposta não tenha controle direto ou indireto sobre a sociedade.

INFORMAÇÃO RELEVANTE

É proibido negociar com informações privilegiadas, a menos que as informações não sejam consideradas relevantes. "Informações relevantes" geralmente são definidas como informações para as quais há uma probabilidade substancial de que um investidor as consideraria importantes ao tomar suas decisões de investimento, ou informações que são razoavelmente certas de terem um efeito substancial no preço de um ativo.

Embora não haja uma definição precisa e geralmente aceita para "informações relevantes", as informações serão consideradas "relevantes" se estiverem relacionadas a mudanças significativas que afetem questões como:

- expectativas de dividendos ou lucros;
- baixas ou perdas de ativos;
- expansão ou redução das operações da empresa ou da divisão principal;
- propostas ou acordos envolvendo joint venture, fusão, aquisição;
- alienação ou aquisição alavancada;
- novos produtos ou serviços;
- desenvolvimentos exploratórios, de descoberta ou de pesquisa;
- acusações criminais, litígios civis ou investigações governamentais;
- disputas com os principais fornecedores ou clientes ou mudanças significativas em as relações tais partes;
- disputas trabalhistas, incluindo greves ou bloqueios;
- mudanças substanciais nos métodos contábeis;
- principais desenvolvimentos de litígios;
- grandes mudanças de equipe;
- dívida ou problemas de liquidez;
- falência ou insolvência;
- desenvolvimentos extraordinários de gestão;
- ofertas públicas ou vendas privadas de títulos de dívida ou de capital;
- chamadas, resgates ou compras de ações da própria empresa;
- ofertas de compra do emissor; ou
- recapitalizações

As informações fornecidas por uma empresa podem ser relevantes devido ao efeito esperado em uma classe específica de títulos da empresa, todos os títulos da empresa, títulos de outra empresa ou títulos de várias empresas. Além disso, a proibição resultante contra o uso indevido de informações "privilegiadas" atinge todos os tipos de títulos (sejam ações ou outras participações societárias, dívida corporativa, obrigações governamentais ou municipais), bem como qualquer opção relacionada a esse título (como uma opção de compra ou venda).

INFORMAÇÃO NÁO-PÚBLICA

Para que surjam questões relativas ao uso de informações privilegiadas, as informações não devem ser apenas "privilegiadas", mas sim "não-públicas". Informações "não-públicas" são informações que não foram disponibilizadas aos investidores em geral. As informações recebidas em circunstâncias que indiquem que ainda não estão em circulação geral ou em que o destinatário saiba ou deva saber que as informações só poderiam ter sido fornecidas por um "*insider*" também são consideradas informações "não-públicas".

No momento em que as informações privilegiadas não-públicas são efetivamente distribuídas ao público, elas não estão mais sujeitas às restrições de uso de informações privilegiadas. No entanto, para que informações "não-públicas" se tornem informações públicas, elas devem ser disseminadas por meio de canais de distribuição reconhecidos, projetados para atingir o mercado de valores mobiliários.

Para mostrar que as informações relevantes são públicas, você deve ser capaz de apontar algum fato para verificar se as informações se tornaram disponíveis, por exemplo, divulgação em uma agência nacional de notícias e notícias financeiras, um noticiário nacional, um jornal nacional, ou um documento de divulgação divulgado publicamente.

A circulação de boatos, mesmo que precisos, difundidos e veiculados na mídia, não constitui a divulgação pública necessária. As informações não devem ser apenas divulgadas publicamente, mas também deve haver tempo adequado para o mercado como um todo digerir as informações

Embora o tempo possa variar dependendo das circunstâncias, uma boa regra prática é que as informações são consideradas não públicas até o terceiro dia útil após a divulgação pública.

As informações relevantes não-públicas não são tornadas públicas por meio de disseminação seletiva. As informações relevantes divulgadas indevidamente apenas a investidores institucionais ou a um analista de fundos ou um grupo de analistas favorecido mantêm seu status como informações "não-públicas" que não devem ser divulgadas ou de outra forma mal utilizadas. Da mesma forma, a divulgação parcial não constitui divulgação pública. Contando que qualquer componente material das informações "privilegiadas" possuídas pela Empresa ainda não tenha sido divulgado publicamente, as informações são consideradas "não-públicas" e seu uso indevido está proibido.

É possível que uma ou mais Pessoas expostas possam se tornar "*insiders*" temporários por exercer uma atividade de confiança. Um atividade de confiança pode surgir: (1) sempre que uma pessoa concorda em manter as informações em sigilo; (2) quando duas pessoas têm um histórico, padrão ou prática de compartilhar confidências de tal forma que o destinatário da informação sabe ou deveria razoavelmente saber que a pessoa que comunica a informação material não pública espera que o destinatário mantenha sua confidencialidade; ou (3) sempre que uma pessoa recebe ou obtém informações materiais não públicas de certos parentes próximos, como cônjuges, pais, filhos e irmãos. Por exemplo, o funcionário da Empresa pode se tornar *insiders* quando uma fonte externa, como um fundo de investimento monitorado pela Empresa, divulga informações materiais não-públicas sobre uma de suas empresas de portfólio para os profissionais de investimento ou um Gerente de Relacionamento com a expectativa de que as informações permanecerão confidenciais.

Como um "insider", a Empresa tem o dever de não violar a confiança da parte que comunicou as informações "relevantes não-públicas" por meio do uso indevido dessas informações. Esta obrigação pode surgir porque a Empresa tem uma relação comercial com o fundo de investimento ou empresa do portfólio e recebeu acesso a informações confidenciais apenas para os fins comerciais desse fundo ou empresa e os clientes da Empresa ou clientes em potencial.

Os membros do Departamento de Investimentos devem ser especialmente cautelosos com informações "relevantes não-públicas" divulgadas em violação do dever de confiança que ele deve à

empresa e aos acionistas. Mesmo quando não há expectativa de confidencialidade, uma pessoa pode se tornar um "*insider*" ao receber informações materiais não públicas em circunstâncias em que uma pessoa sabe, ou deveria saber, que um "*insider*" corporativo está divulgando informações em violação de um cargo de confiança.

A divulgação de uma "dica" imprópria torna o destinatário um favorecido se o "*insider*" corporativo espera se beneficiar pessoalmente, direta ou indiretamente, com a divulgação. No contexto de uma divulgação indevida por um "*insider*" corporativo, o requisito "benefício pessoal" não pode ser limitado a um ganho monetário presente ou futuro.

Uma pessoa pode, dependendo das circunstâncias, também se tornar um "*insider*" ou "favorecido" quando obtém informações aparentemente materiais e não-públicas por acaso, incluindo informações derivadas de situações sociais, reuniões de negócios, conversas ouvidas, documentos extraviados, e "dicas" de internos ou de terceiros.

IDENTIFICAÇÃO DE INFORMAÇÃO RELEVANTE

As pessoas expostas devem fazer a si mesmas as seguintes perguntas antes de negociar para suas próprias contas ou contas de outros valores mobiliários de uma empresa sobre a qual possam ter informações relevantes não-públicas:

I. Essas informações podem ser consideradas relevantes por um investidor na tomada de decisões de investimento? Essas informações podem afetar substancialmente o preço de mercado dos valores mobiliários, se divulgadas de maneira geral?
II. A quem esta informação foi fornecida? As informações foram comunicadas de forma eficaz ao mercado ao serem publicadas veículos de circulação geral?

Dadas as sanções regulatórias, civis e criminais potencialmente graves às quais a Empresa e seu funcionários podem estar sujeitos, qualquer Pessoa exposta em dúvida se as informações que possui são informações "relevantes não-públicas" deve tomar imediatamente as seguintes medidas:

I. Reportar imediatamente ao Diretor de Compliance
II. Não compra ou vender os títulos por contas próprias ou de terceiros; e
III. Não divulgar as informações dentro ou fora da Empresa, a não ser para o Departamento de Compliance.

Após o Diretor de Compliance analisar a situação, a Pessoa exposta poderá ser instruída a continuar com as proibições de negociação e comunicação ou terá permissão para negociar e comunicar as informações.

PENALIDADE PARA "INSIDER TRADING"

As penalidades por negociar ou comunicar informações relevantes não públicas são severas, tanto para os indivíduos envolvidos em tal conduta ilegal quanto para seus favorecidos. Uma pessoa pode estar sujeita a algumas ou todas as penalidades abaixo, mesmo que ela não se beneficie pessoalmente da violação. As penalidades incluem injunções civis, danos triplos, devolução de lucros, sentenças de prisão, multas para a pessoa que cometeu a violação de até três vezes o lucro ganho ou perda evitada, sendo a pessoa realmente beneficiada ou não, e multas para o empregador ou outra entidade controladora.

Além disso, pode-se esperar que qualquer violação desta declaração de política resulte em sérias sanções por parte da Empresa, incluindo a demissão das pessoas envolvidas

PROCEDIMENTOS PARA IMPLEMENTAR A POLÍTICA DE "INSIDER TRADING"

Os procedimentos a seguir foram estabelecidos para ajudar as pessoas expostas a evitar acesso a informações privilegiadas e para ajudar a Empresa a prevenir, detectar e impor sanções contra uso de informações privilegiadas. Cada pessoa exposta deve seguir estes procedimentos ou corre o risco de sanções graves, incluindo demissão e penalidades criminais.

Nenhuma Pessoa exposta que tenha conhecimento de informações relevantes não-públicas relacionadas a qualquer outra empresa ou entidade em circunstâncias em que tal pessoa seja considerada uma pessoa exposta ou esteja sujeita a restrições sob as leis pode comprar ou vender títulos dessa empresa ou de outra forma tirar vantagem de, ou repassar a terceiros, tais informações relevantes não-públicas. As informações privilegiadas podem ser comunicadas apenas aos funcionários da Empresa que tenham necessidade de conhecê-las no desempenho de suas funções.

As pessoas expostas deverão apresentar relatórios sobre cada transação com valores mobiliários de acordo com a política para negociação pessoal.

Porque mesmo a divulgação inadvertida de informações relevantes não-públicas a terceiros pode levar a implicações legais significativas, as Pessoas expostas não devem discutir quaisquer informações não-públicas potencialmente materiais relativos à Empresa ou outras empresas, incluindo outras Pessoas expostas, exceto conforme especificamente exigido no desempenho de suas funções.

PROCEDIMENTOS DE SEGURANÇA

É exigido o estabelecimento e a aplicação estrita de procedimentos razoavelmente projetados para prevenir o uso indevido de informações "privilegiadas". Consequentemente, não devem ser discutidas informações relevantes não-públicas sobre a Empresa ou outras empresas com ninguém, incluindo outras Pessoas expostas, exceto conforme exigido no desempenho de suas funções regulares. Além disso, deve-se ter cuidado para que essas informações sejam seguras. Por exemplo, o acesso a arquivos de computador contendo informações relevantes não-públicas deve ser restrito.

RESOLUÇÃO DE QUESTÕES RELATIVAS AO "INSIDER TRADING"

Qualquer pessoa exposta que tiver dúvidas quanto à materialidade ou natureza não pública das informações em sua posse ou quanto à aplicabilidade ou interpretação de qualquer um dos procedimentos anteriores ou quanto à propriedade de qualquer ação deve entrar em contato com o Departamento de Compliance. Até que sejam informadas em contrário por um membro do Departamento de Compliance, as pessoas expostas devem presumir que as informações são relevantes e não-públicas e não devem negociar os valores mobiliários ou divulgar essas informações a ninguém.

PREVENÇÃO AO "INSIDER TRADING"

Para evitar a ocorrência de uso de informações privilegiadas, o Departamento de Compliance deve:

I. garantir que todos os funcionários e pessoas expostas estejam familiarizados com a política da Empresa;
II. Responder a perguntas e dúvidas sobre a política da Empresa;
III. Revisar a política da Empresa regularmente e atualizá-la conforme necessário para refletir as mudanças regulatórias e da indústria;
IV. Identificar se as informações recebidas por uma Pessoa exposta constituem informações relevantes e não públicas;
V. se necessário, manter e atualizar uma "lista de observação" para monitorar e prevenir a ocorrência de negociações com uso de informações privilegiadas em certos valores mobiliários que a Empresa está proibida ou restrita de negociar; e,
VI. Conduzir reuniões periódicas com todos os funcionários para revisão da política

DETECÇÃO DE "INSIDER TRADING"

A fim de detectar o uso de informações privilegiadas, o Departamento de Compliance deve:

I. revisar os relatórios de atividades de investimentos submetidos por cada Pessoa exposta; e
II. revisar registros de operações financeiras e outras informações relevantes; e
III. revisar transações que podem exigir análise adicional ou acompanhamento.

SIGNAL
CAPITAL

POLÍTICA DE PLD/FTP

OBJETIVO

A Signal Capital, juntamente com os Fundos sob sua gestão está comprometida em cumprir todas as leis e regulamentos aplicáveis de combate à lavagem de dinheiro, ao financiamento do terrorismo e da proliferação de armas de destruição em massa ("PLD/FTP") e envidará seus melhores esforços para minimizar a ameaça de tais atividades, através da implementação de um programa destinado a detectar, prevenir e coibir tais crimes.

A lavagem de dinheiro é o processo pelo qual criminosos ocultam a existência, natureza ou origem de fundos que derivam de atividades criminosas ou que foram obtidos por meios corruptos. Frequentemente, o dinheiro obtido ilegalmente é aplicado em instituições financeiras legítimas ou na economia geral, convertendo-o em outros ativos, separando-o de sua fonte original, ocultando, assim, sua origem ilegal. Nesse sentido, as instituições financeiras desempenham papel importante no combate a esse ilícito, na medida em que podem impedir que ilegalidades ocorram, uma vez identificadas situações sobre as quais recaiam suspeitas de LD/FTP.

Desse modo, as leis e regulamentos de PLD/FTP atribuem às instituições financeiras uma série de deveres que visam à prevenção do cometimento e à mitigação dos efeitos de tais crimes. Entre as diversas exigências legais sobre os fundos privados, por exemplo, estão a necessidade de relatar transações envolvendo dinheiro e certos instrumentos negociáveis e de comunicar atividades financeiras suspeitas por parte de clientes da Empresa ou investidores nos Fundos da Empresa. Ainda é recomendado que a Empresa e seus Fundos evitem estabelecer ou continuar relações comerciais com quaisquer indivíduos, empresas e outras entidades de reputação duvidosa.

No atendimento a estas exigências, a Signal Capital irá adotar uma série de medidas, descritas ao longo deste documento, envolvendo os diversos atores com os quais a Empresa interage no curso de sua atividade. Esta Política de PLD/FTP faz parte desse esforço, cumprindo tanto a função de delinear as responsabilidades e processos relacionados ao combate a tais crimes quanto a de educar os funcionários da Signal Capital no que diz respeito à PLD/FTP.

APROVAÇÃO E ADMINISTRAÇÃO DA POLÍTICA

A responsabilidade pela aprovação da Política de PLD/FTP cabe à alta administração da Signal Capital, representada por sua Diretoria.

O Diretor de Compliance é responsável por implementar e monitorar a conformidade geral com a política de PLD/FTP. O Diretor de Compliance tem autoridade total para implementar e fazer cumprir

a política de PLD/FTP. Todas as questões relativas às políticas e procedimentos de PLD/FTP devem ser dirigidas ao Diretor de Compliance.

O Diretor de Compliance deve ter independência, autonomia e conhecimento técnico suficiente para o pleno cumprimento dos seus deveres, assim como amplo, irrestrito e tempestivo acesso a todas as informações que julgar necessárias para que a respectiva governança de riscos de LD/FTP possa ser efetuada. O Diretor pode desempenhar a função em conjunto com outras atividades na instituição, desde que não haja conflitos de interesses entre elas.

As responsabilidades do Diretor de Compliance incluem:

I. garantir a conformidade entre o programa de PLD/FTP da Signal Capital e as leis e regulamentações vigentes;
II. implementar e acompanhar o cumprimento da política, regras, procedimentos e controles de PLD/FTP, de modo a assegurar o efetivo gerenciamento dos riscos relacionados;
III. difundir a cultura de PLD/FTP entre os colaboradores, inclusive por meio da adoção de programas periódicos de treinamento;
IV. determinar quais pessoas serão obrigadas a receber treinamento para continuidade do programa de PLD/FTP da Signal Capital;
V. supervisionar o treinamento periódico;
VI. coletar relatórios de atividades suspeitas preparados por funcionários da empresa, auxiliando-os na revisão de tais relatórios, e na avaliação e investigação de tais atividades;
VII. elaborar relatório relativo à Avaliação Interna de Risco de LD/FTP, a ser encaminhado para a Diretoria da Signal Capital;
VIII. informar os funcionários de todas as mudanças nas políticas, procedimentos e controles da Signal Capital quando feitas em resposta à evolução da legislação e dos regulamentos à medida que são propostos e adotados;
IX. comunicar ao Coaf (Conselho de Controle de Atividades Financeiras) as operações ou propostas de operações que possam constituir-se em sérios indícios de LD/FTP;
X. comunicar à CVM, se for o caso, a não ocorrência, no ano civil anterior, de situações, operações ou propostas de operações passíveis de serem comunicadas;
XI. coordenar ações disciplinares a serem aplicadas a colaboradores e prestadores de serviços que venham a descumprir os procedimentos de PLD/FTP; e
XII. avaliar regularmente o programa de PLD/FTP, de modo a garantir sua eficiência e efetividade.

INDÍCIOS DE LD/FTP

São diversos os sinais de que se pode estar diante de uma tentativa ou efetiva lavagem de dinheiro. A fim de tornar mais tangível de que forma esse crime se manifesta no contexto da rotina de um fundo privado, trouxemos alguns exemplos.

Podem configurar indícios de LD/FTP, a título de exemplo: a impossibilidade de manter atualizadas as informações cadastrais de clientes ou de identificar o beneficiário final; situações em que as diligências relativas ao processo de conhecimento dos clientes não possam ser concluídas; operações realizadas entre as mesmas partes ou em benefício das mesmas partes, nas quais haja seguidos ganhos ou perdas para algum dos envolvidos; operações cujo grau de complexidade e risco se afigurem incompatíveis com o perfil do cliente ou com seu porte ou objeto social; entre outras, nos termos do art. 20 e incisos da Resolução CVM nº. 50/21.

PROCESSOS E CONTROLES

A Signal Capital deverá, no limite de suas atribuições, identificar, analisar, compreender e mitigar os riscos de LD/FTP ("Avaliação Interna de Risco"), adotando uma abordagem baseada em risco ("ABR"), a fim de assegurar que as medidas de prevenção e mitigação sejam proporcionais aos riscos identificados. Nesse sentido, a Signal Capital deve elencar todos os produtos oferecidos, serviços prestados, respectivos canais de distribuição e ambientes de negociação e registro, segmentando-os em "baixo", "médio" e "alto" risco de LD/FTP; e classificar os respectivos clientes por grau de risco de LD/FTP, segmentando-os em "baixo", "médio" e "alto" risco.

A Avaliação Interna de Risco deve envolver as seguintes categorias de risco:

a. perfil de risco do cliente;
b. perfil de risco da instituição, incluindo o modelo de negócio e a área geográfica de atuação;
c. perfil de risco das operações, transações, produtos e serviços prestados, abrangendo todos os canais de distribuição e a utilização de novas tecnologias;
d. perfil de risco das atividades exercidas pelos colaboradores e prestadores de serviços;
e. perfil de risco dos canais de distribuição e ambientes de negociação e registro; e
f. perfil de risco relativo ao relacionamento da instituição com outras pessoas submetidas à regulação de PLD/FTP da CVM.

O relatório de Avaliação Interna de Risco de LD/FTP, a ser elaborado anualmente pelo Diretor de Compliance, deve ser encaminhado para a Diretoria da Signal Capital até o último dia útil do mês de abril, contendo identificação e análise das situações de risco de LD/FTP, considerando as respectivas ameaças, vulnerabilidades e consequências; a apresentação de recomendações visando mitigar os riscos identificados no exercício anterior; e outras informações que o Diretor de Compliance julgar pertinentes, em conformidade com o art. 6º e incisos da Resolução CVM nº. 50/21.

Em paralelo à produção de um relatório de Avaliação Interna de Risco, a Signal Capital deve monitorar continuamente todas as operações e situações que a ela se apresentam, devendo a análise destas ser feita de acordo com procedimentos regulares e tempestivos, a fim de identificar aquelas que configurem indícios de LD/FTP. É dever dos colaboradores da Signal Capital relatar qualquer indício

de situação atípica de LD/FTP ao Diretor de Compliance, devendo ele comunicar ao COAF todas as situações, operações ou propostas de operações que, mediante análise fundamentada, possam constituir-se em sérios indícios de LD/FTP.

A conclusão das análises oriundas do monitoramento deve ocorrer em até 45 (quarenta e cinco) dias contados da data do alerta, devendo a comunicação ao Coaf ser feita dentro de 24 horas contadas da conclusão da análise que caracterizou a atipicidade da operação, da respectiva proposta ou mesmo da situação atípica detectada.

O processo de análise de clientes e transações deve considerar, entre outros fatores, a origem e o destino dos recursos; a reincidência do desenquadramento de perfil histórico de transações; a relação da movimentação com o atual comportamento do mercado; e notícias desabonadoras na mídia e verificação de listas restritivas.

Com vistas a coibir a LD/FTP sob a ótica dos clientes e investidores, pode-se adotar tanto medidas direcionadas a novos clientes quanto ações que tem foco nos clientes já compõem a base da Signal Capital. Todos os novos clientes da Signal Capital e investidores em qualquer um de seus Fundos (incluindo aqueles que se tornam investidores devido à transferência de cotas de um investidor existente) serão obrigados a fazer representações e garantias com relação a questões de PLD/FTP e incorporar os respectivos contratos de assessoria de investimento ou gestão de investimentos (no caso de clientes) ou documentos de subscrição ou transferência (no caso de investidores Fundos da Signal Capital); sendo, no entanto, reservada ao Diretor de Compliance a faculdade de modificar ou dispensar esse requisito se, com base nas informações disponíveis ao Diretor de Compliance em relação ao cliente ou investidor em potencial, tais representações, garantias e convênios forem desnecessários.

Antes de aceitar um novo cliente ou admitir um novo investidor para um Fundo da Signal Capital, ou consentir com a transferência da participação de um investidor existente para um novo investidor, o Diretor de Compliance deve determinar se o investimento representa um risco de lavagem de dinheiro e, em caso afirmativo, deve procurar, na medida do razoável e praticável, assegurar que tal admissão ou transferência não seja para fins de lavagem de dinheiro. Para esse fim, os funcionários apropriados devem fazer esforços para verificar a identidade de uma instituição, incluindo nome, endereço, entidade legal e outras informações de identificação aplicáveis para determinar a fonte do capital do investidor. Em prol desse objetivo, e na medida do aplicável, a Signal Capital também mantém arquivos de PLD/FTP relacionados à documentação solicitada, incluindo, mas não se limitando a, acordos de confiança ou documentos reguladores semelhantes, certificados, documentos constitutivos de personalidade jurídica e resoluções. O Diretor de Compliance está autorizado a modificar ou dispensar este requisito nas circunstâncias descritas acima.

Esforços também devem ser realizados para confirmar que a aceitação de um novo cliente ou a admissão de um novo investidor em um Fundo da Signal Capital ou um cessionário de uma posição de investidor existente não se destina a facilitar atividades de lavagem de dinheiro ou não constitui um investimento proibido. Um investimento é proibido quando realizado por qualquer pessoa ou entidade agindo, direta ou indiretamente, em violação de quaisquer leis e regulamentos de PLD/FTP ou em nome de terroristas ou organizações terroristas, incluindo aqueles que estão incluídos em quaisquer listas de vigilância relevantes. Consequentemente, esta política exige que o Diretor de Compliance ou funcionários apropriados designados pelo Diretor de Compliance consultem listas de terroristas ou organizações terroristas conhecidas ou suspeitos, comparem-nas com as informações fornecidas por clientes ou investidores quanto a seus nomes, país de origem e assuntos relacionados, e relatem suas conclusões ao Diretor de Compliance. Determinadas agências governamentais restringiram as instituições financeiras de se envolverem em transações financeiras com os indivíduos, entidades, grupos, organizações e países designados em tais listas, bem como quaisquer outras listas que possam ser exigidas por lei ou regulamento. A Signal Capital poderá utilizar o World-Check e o LexisNexis como parte de seus esforços de PLD/FTP. Esses serviços oferecem um banco de dados de indivíduos e empresas de alto risco conhecido, derivados de várias fontes públicas, incluindo combate à lavagem de dinheiro e listas de vigilância de terroristas emitidas por governos nacionais.

Os funcionários relevantes também serão orientados a monitorar atividades incomuns ou suspeitas por parte de qualquer cliente ou investidor de Fundos da Signal Capital e relatá-las imediatamente ao Diretor de Compliance. As atividades suspeitas incluem o pagamento de taxas à Signal Capital ou contribuições de capital para um Fundo da Signal Capital em dinheiro, instrumentos semelhantes a dinheiro (ordens de pagamento, cheques de viagem, cheques bancários) ou cheques de terceiros, falha ou falta de vontade de fornecer informações sobre o cliente ou negócios do investidor ou outras informações de que a empresa precisa para cumprir as leis e regulamentos de PLD/FTP, fornecendo documentos corporativos ou de identificação incomuns ou duvidosos, ou mostrando preocupação com as obrigações da empresa em cumprir os requisitos de relatórios do governo e cooperar com os encarregados da aplicação da lei.

Restrições devem ser impostas aos meios usados para transferir recursos de e para os Fundos da Signal Capital, e as distribuições aplicáveis dos Fundos da Signal Capital devem ser feitas apenas ao detentor da posição do investimento conforme identificado registros do Fundo, a menos que aprovado de outra forma pelo Diretor de Compliance.

TREINAMENTO

A Signal Capital irá educar e treinar, sob a supervisão do Diretor de Compliance, todos os funcionários relevantes, administradores, sócios, estagiários, terceirizados e prestadores de serviços, quando aplicável, sobre como prevenir a LD/FTP. Estes serão completamente informados sobre o programa de PLD/FTP da Signal Capital e suas obrigações legais sob as leis e regulamentos de PLD/FTP

aplicáveis, sendo responsáveis por tomar todas as medidas razoáveis e práticas para ajudar a Signal Capital e seus Fundos a implementar e cumprir esta política. O não cumprimento desta política pode resultar em medidas disciplinares, rescisão do contrato de trabalho e penalidades civis e criminais, tanto para os indivíduos quanto para a Signal Capital e seus Fundos.

O Departamento de Compliance, por meio de treinamento anual, deve discutir os procedimentos e controles que estão sendo implementados pela Signal Capital para garantir que os funcionários e pessoas com acesso os entendam. O Departamento de Compliance deve modificar e complementar o programa de treinamento conforme necessário e conforme os regulamentos de implementação das leis de PLD/FTP são propostos e adotados; deve informar imediatamente todos os funcionários afetados e pessoas com acesso das informações de treinamento atualizadas; e deve fornecer treinamento contínuo em todos os procedimentos e controles, novos e existentes.

PROCEDIMENTOS "CONHEÇA SEU CLIENTE, COLABORADOR E PRESTADOR DE SERVIÇO"

No que diz respeito ao procedimento "conheça seu cliente", enquanto Gestor de fundos de investimento com múltiplos cotistas, não envolvido na distribuição das cotas desses fundos, para fins do Ofício-Circular nº 4/2020-CVM/SMI-SIN, a Signal Capital tem como clientes os próprios fundos de investimento. Nesse sentido, cabe à Signal Capital apenas obter os dados cadastrais dos fundos previstos no anexo B à Resolução CVM 50/21.

No que tange ao procedimento "conheça seu colaborador", a Signal Capital irá considerar o risco de LD/FTP das atividades desempenhadas, a posição que os colaboradores ocupam, inclusive seu histórico profissional, de forma a verificar se o colaborador possui envolvimento com crimes financeiros, lavagem de dinheiro ou outros delitos similares. O referido procedimento não se encerrará no momento da contratação, devendo a Signal Capital ficar atenta ao comportamento dos colaboradores, de modo a detectar e subsequentemente relatar possíveis atividades atípicas, tais como ações e condutas não compatíveis com seu padrão de vida, remuneração ou conduta pregressa.

Já no que concerne ao procedimento "conheça seu prestador de serviço", a Signal Capital irá verificar se os prestadores de serviço em potencial e presentes possuem políticas e práticas de PLD/FTP compatíveis com as que a própria instituição adotaria em seu lugar. O procedimento, ainda, será implementado de acordo com a atividade contratada, o risco de LD/FTP que ela representa e o propósito de relacionamento com o prestador, seguindo os princípios da razoabilidade e do bom senso. Uma vez conhecido o prestador de serviço, a Signal Capital deve classificá-lo de acordo com seu grau de risco.

INTERCÂMBIO DE INFORMAÇÕES

A Signal Capital não se absterá, para fins de cumprimento das regras de PLD/FTP, sobretudo nas operações e situações de maior risco, de utilizar-se do compartilhamento de informações – inclusive sobre cotistas diretos e indiretos – entre prestadores de serviços dos fundos de investimento, notadamente administradores fiduciários, gestores de recursos, custodiantes e distribuidores, tendo em vista a orientação da CVM no sentido de uma interpretação sistemática e teleológica da Lei Complementar 105/01, das Leis nº. 9.613/98, nº. 13.260/16, nº. 13.810/19 e da LGPD.

REVISÕES E ATUALIZAÇÕES

A Signal Capital deve avaliar a efetividade de seus procedimentos e controles de PLD/FTP a partir de indicadores de efetividade, de forma periódica, apresentando-os no relatório de Avaliação Interna de Risco da empresa. O Programa de PLD/FTP da Signal Capital deve ser atualizado de tempos em tempos, conforme necessário, em resposta às novas regras e regulamentos à medida que são propostos e adotados.

PLANO DE CONTIGÊNCIA

OBJETIVO

O Diretor de Compliance é responsável por desenvolver procedimentos escritos para iniciar uma recuperação oportuna de um desastre ou outro evento que resulte na interrupção dos negócios da Empresa. A base desses procedimentos é minimizar o impacto de um desastre ou outro evento semelhante para a Empresa, seus funcionários e clientes.

O plano deve conter:

- Quem pode declarar uma emergência;
- Quem é responsável por manter uma lista de contatos de funcionários;
- Local de reunião primário e secundário se o escritório principal for destruído ou não puder ser usado;
- Notificação às autoridades regulatórias competentes sobre a emergência e sua natureza;
- Recuperação de informações do cliente;
- Backup de sistema de comunicação/telefone para clientes, pessoal e outros para possibilitar o contato com a Empresa e para a Empresa contatar clientes;
- Realizar testes periódicos e anuais do plano em condições simuladas e treinamento de todo o pessoal crítico.